COMMON VULNERABILITIES IN CLOUD ENVIRONMENTS

Swipe

CLOUD MISCONFIGURATIONS

Cloud misconfigurations are a major security risk. These misconfigurations can allow attackers to gain unauthorized access to cloud resources or sensitive data.

common cloud misconfigurations:

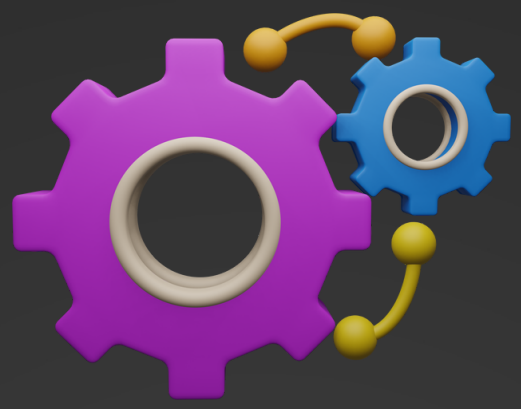
- Using default passwords or keys
- Leaving unused accounts enabled
- Exposing sensitive data to the public internet
- Not using strong encryption

WEAK ACCESS CONTROLS

Weak access controls are another major security risk in cloud environments. These weak controls can allow unauthorized users to gain access to sensitive data or systems.

Common weak access controls:

- Using shared passwords
- Not requiring multi-factor authentication
- Not rotating passwords regularly



OUTDATED SOFTWARE

Outdated software is often vulnerable to attack. Cloud environments must be kept up-to-date with the latest security patches.

Common outdated software vulnerabilities:

- Vulnerabilities in operating systems
- Vulnerabilities in web applications
- Vulnerabilities in cloud management tools

DATA BREACHES

Cloud environments are often used to store sensitive data. If this data is not properly protected, it could be exposed in a data breach. Data breaches can have a significant impact on an organization's reputation and bottom line.

DENIAL-OF-SERVICE (DOS) ATTACKS

DoS attacks can overwhelm a cloud environment with traffic, making it unavailable to legitimate users. DoS attacks can be launched from anywhere in the world and can be difficult to defend against.

ZERO-DAY ATTACKS

Zero-day attacks exploit vulnerabilities that are unknown to the software vendor. These attacks can be very difficult to defend against because there is no patch available to fix the vulnerability.

DON'T LET CLOUD SECURITY VULNERABILITIES PUT YOUR BUSINESS AT RISK.

GET A CLOUD SECURITY AUDIT FROM OUR EXPERTS

BRISK INFOSEC
CYBER TRUST & ASSURANCE

Your Perfect Cybersecurity Partner

+91 7305979769

contact@briskinfosec.com